6th International Conference on
Combinatorics, Cryptography, Computer Science and Computing
November. 17-18, 2021

A Class of Column-weight-3 Quasi-Cyclic Low-Density Parity-Check Codes from Greatest Common Divisor

Marjan Majdzade[1]
Iran University of Shahrekord, Shahrekord, Iran

Mohammad Gholami
Shahrekord University, Shahrekord, Iran

Abstract

A (type-I) quasi-cyclic low-density parity-check (QC-LDPC) code can be described by a *circulant permutation matrix* (CPM) size and an *exponent matrix* whose entries are non-negative integers not greater than the CPM-size.

For any column weight J and any row weight L, a novel framework has been proposed recently such that a girth-eight (J,L) QC-LDPC code with CPM-size above a lower bound can be constructed via a simple inequality in terms of greatest common divisor (GCD). In this paper, using this GCD condition, an explicit method to generate of a class of girth-8 column weight-3 of a QC-LDPC code is proposed.

Keywords: QC-LDPC codes, explicit constructions, girth, exponent matrix.

Mathematics Subject Classification [2010]: 13D45, 39B42

1 Introduction

QC-LDPC codes are an important class of LDPC codes that are preferred on other types of LDPC codes because of their practical and simple implementations [2]. By a (J, L) QC-LDPC code with CPM-size P, we mean a linear code whose parity-check matrix (PCM) is a $J \times L$ array of circulant permutation matrices (CPMs) of size P. In fact, a (J, L) QC LDPC code can be described by a CPM-size P and a $J \times L$ matrix, called *exponent matrix*, of some non-negative integers less than P. In this case, if $E = (e_{i,j})$ is the exponent matrix, the corresponding QC-LDPC code is described by its PCM constructed by replacing each entry $e_{i,j}$ of E by CPM $\mathcal{I}^{e_{i,j}}$, in which $\mathcal{I}^{e_{i,j}}$ is obtained from the identity matrix by cyclically shifting each column up by $e_{i,j}$ positions to the left.

One of the most important models to represent an LDPC code with PCM H, is Tanner graph [1], TG(H), which is a bipartite graph collecting variable and check nodes associated to the columns and rows of H, respectively, and a check node is connected to a variable node, if a nonzero entry exists in the intersection of the corresponding row and column. The length of the shortest cycles of the Tanner graph, girth, has been known to influence the code performance and the error correction and detection are improved by enlarging the girth [6]. In general, LDPC codes with large girth and small number of short cycles have good performances [8], so lots of efforts have been put into constructing codes with large girth [4]-[7].

[1]speaker

2 Preliminaries

A (J, L) (Type-I) QC-LDPC code with *exponent matrix* $E = (e_{i,j})$ and CPM-size P can be described by the parity-check matrix $H = (H_{i,j})_{1 \le i \le J, 1 \le j \le L}$, in which $H_{i,j} = \mathcal{I}^{e_{i,j}}$ is obtained from the $P \times P$ identity matrix by cyclically shifting each column up by $e_{i,j}$ positions to the left. Hereinafter, we consider (J, L) QC-LDPC codes with the following exponent matrix.

$$E(a_0, a_1, \cdots, a_{J-1}) = \begin{pmatrix} a_0.0 & a_0.1 & \dots & a_0.(L-1) \\ a_1.0 & a_1.1 & \dots & a_1.(L-1) \\ \vdots & \vdots & \ddots & \vdots \\ a_{J-1}.0 & a_{J-1}.1 & \dots & a_{J-1}.(L-1) \end{pmatrix} \quad (1)$$

where $a_0, a_1, \cdots, a_{J-1}$ is a finite sequence of non-negative integers with $a_0 < a_1 \cdots < a_{J-1}$. In [5], a sufficient condition, called *GCD condition*, is provided for the code with exponent matrix (1) to have girth at least 8 as follows.

GCD condition. If $(a_k - a_i)/\gcd(a_k - a_i, a_j - a_i) \ge L$ for all (a_i, a_j, a_k), $0 \le i < j < k \le J - 1$, then the (J, L) QC-LDPC code with exponent matrix $E(a_0, a_1, \cdots, a_{J-1})$ has girth at least 8 for each CPM-size $P \ge (a_{J-1} - a_0)(L - 1) + 1$.

3 A class of girth-8 $(3, L)$ QC-LDPC codes

In this section we need to a triple (a_0, a_1, a_2) satisfied in GCD condition to construct a QC-LDPC code with girth 8. First, let $\Gamma(L)$ is the set of non-negative integers less than L that are relatively prime to L.

Lemma 3.1. *Suppos $a_0 = 0$, $a_2 = L$ and $a_1 \in \Gamma(L)$. Then,the $3 \times L$ exponent matrix $E(0, a_1, L)$ corresponds to a girth-eight Tanner graph for any CPM-size $P \ge L(L - 1) + 1$.*

Proof. Using GCD condition, to have a QC-LDPC code with girth 8, the condition $(a_2 - a_0)/\gcd(a_2 - a_0, a_1 - a_0) \ge L$ must be satisfied for $a_0 = 0$, $a_2 = L$ and $a_1 \in \Gamma(L)$. In this case $L/\gcd(L, a_1) \ge L$ and due to $a_1 \in \Gamma(L)$, $\gcd(L, a_1) = 1$. Therefore the GCD condition holds and $E(a_0, a_1, a_2)$ corresponds to a QC-LDPC code with girth 8 for any $P \ge (a_2 - a_0)(L - 1) + 1 = L(L - 1) + 1$. □

As a result, Lemma (3.1) includes the cases $(0, L-1, L)$ and $(0, 1, L)$ which is mentioned in [5] i.e Lemma (3.1) is more general.

Example 3.2. Let the following exponent matricies:

$$E(0,1,8) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 8 & 16 & 24 & 32 & 40 & 48 & 56 \end{pmatrix}$$

$$E(0,3,8) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 6 & 9 & 12 & 15 & 18 & 21 \\ 0 & 8 & 16 & 24 & 32 & 40 & 48 & 56 \end{pmatrix}$$

$$E(0,5,8) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 5 & 10 & 15 & 20 & 25 & 30 & 35 \\ 0 & 8 & 16 & 24 & 32 & 40 & 48 & 56 \end{pmatrix}$$

$$E(0,7,8) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 7 & 14 & 21 & 28 & 35 & 42 & 49 \\ 0 & 8 & 16 & 24 & 32 & 40 & 48 & 56 \end{pmatrix}$$

Thus, all of the exponent matrices correspond to a QC-LDPC code with girth 8 for any $P > 56$, Because of $a_1 \in \Gamma(8) = \{1, 3, 5, 7\}$ and GCD condition holds.

In a special case if L is a prime number, then for any desired number a_1, $E(0, a_1, L)$ corresponds to a QC-LDPC code with girth 8 for any $P \ge L(L - 1) + 1$ too.

4 Conclusion

Based on greatest common divisor, we have proposed a general construction for girth-eight QC-LDPC codes with column weight 3 and any row weight L with exponent matrix $E(0, a_1, L)$ (such that $a_1 \in \Gamma(L)$) which includes the mentioned cases $E(0, L-1, L)$ and $E(0, 1, L)$ in [5].

Acknowledgment

This work was supported by the research council of Shahrekord University

References

[1] R. M. Tanner, D. Sridhara, and T. E. Fuja (2001), *A class of group-structured LDPC codes*, in Proc. Int. Symp. Commun. Theory Appl., Ambleside, U.K., 365–370.

[2] M. P. C. Fossorier *Quasi-cyclic low-density parity-check codes from circulant permutation matrices*, IEEE Trans. Inform. Theory, 8(50): 1788–1793, 2004.

[3] J. Zhang J, G. Zhang, *Deterministic girth-eight QC-LDPC codes with large column-weight*, IEEE Commun. Lett., 18(4): 656-659, 2014.

[4] G. Zhang, R. Sun, X. Wang, *Several explicit constructions for* $(3, L)$ *QC-LDPC codes with girth at least eight*, IEEE Commun. Lett., 17(9): 1822-1825, 2013.

[5] G. Zhang, R. Sun, X. Wang, *Construction of girth-eight QC-LDPC codes from greatest common divisor*, IEEE Commun. Lett., 17(2): 369–372, 2013.

[6] M. Karimi and A. Banihashemi, *On the girth of quasi cyclic protograph LDPC codes*, IEEE Trans. Inform. Theory, 7(59): 4542–4552 (2013).

[7] M. Majdzade and M. Gholami, *On the Class of High-Rate QC-LDPC Codes with Girth 8 From Sequences Satisfied in GCD Condition*, IEEE Commun. Lett.,7(24): 1391–1394, 2020.

[8] L. Zhang, Q. Huang, S. Lin, K. Abdel-Ghaffar, IF Blake, *Quasi-cyclic LDPC codes: an algebraic construction, rank analysis, and codes on Latin squares*, IEEE Trans. Commun., 58(11): 3126–3139, 2010.

Email: `marjanmajdzade@gmail.com`
Email: `gholami-m@sci.sku.ac.ir`